COMMONWEALTH
of VIRGINIA
Department of Information Technology
110 SOUTH SEVENTH STREET
RICHMOND, VIRGINIA 23219
(804) 371-5000

INTERNET E-MAIL ALERT

To: Security Officers

From: Don Kendrick
Chief Security Architect

Re: "Friendly Greetings" E-Mail

Date: November 5, 2002

DIT has received several updates from TruSecure, a security partner of DIT, regarding the "Friend Greetings" e-mail. This advisory is to make your organization aware of the threat and to recommend appropriate counter measures. This threat appears to affect only users of Outlook and Outlook Express. An additional story appears on MSNBC (<http://www.msnbc.com/news/826033.asp?0cl=cR>) as well as Symantec's site (<http://securityresponse.symantec.com/avcenter/venc/data/friendgreetings.html>).

Description of Threat

In the typical scenario, an e-mail arrives referencing “Friend Greetings”, telling the recipient that that an e-card awaits and providing a link to what appears to be a legitimate e-card website.

After clicking on the link, the user is prompted to download an ActiveX control and a EULA (End User License Agreement) is presented for acceptance. Frequently, users simply accept without reading the EULA, however, buried in the agreement, the user is informed that the control activates Outlook and authorizes the mass mailing of the e-card message to any or all contacts contained in the user’s address book.

Problem

All that appears in the email is some text and an URL, therefore there are no attachments to block, or code for anti-virus software to scan. Further, since it will not do anything without the user's permission (as given, buried in the EULA) there is uncertainty about whether or not anti-virus products will ever detect this sort of activity.

Recommendations

It is recommended that you simply block the whole site (http://www.friendgreetings.com) at your firewall. However, be aware that the people responsible for these attacks periodically change the name/address of the site as things get blocked.

The best advice is to actively block those URL's as discovered, create policy prohibiting e-cards as a non-business use of resources and educate users to delete these emails as received. Please do not hesitate to contact me if I can be of further assistance.

If your machine is infected, removal instructions are available at the Symantec site (<http://securityresponse.symantec.com/avcenter/venc/data/friendgreetings.html>). These instructions include directions for both removal by an anti-virus product as well as manual removal.

Don Kendrick, CNE, CCNA, GCIA, CISSP
Chief Security Architect
Commonwealth of Virginia
Department of Information Technology
(804) 371-5715
110 S. 7th Street
Richmond, Virginia 23219